On the Converse of Lagrange's Theorem

Paul Brennan[17494372], Ronan Timon[17336181]

Groups[MA3343], Lecturer: Rachel Quinlan

Introduction

In Group Theory, a relatively new field of study, few theorems bear the same weight as that of Lagrange's. Only fully proven in 1861 by Camille Jordan, it introduces the notion of an index to the algebra, as well as imbuing Groups with some of the properties that make other forms of algebra so intuitive. However, the theorem's converse is infamously false. We aim to investigate where the theorem fails, but also where it works, and perhaps to find a theorem that works more generally.

Disproving Lagrange's Theorem

A very easy example to demonstrate is that of the group of even permutations, A_4 :

Claim:

If G is a finite group, and

$\exists$ d $\in \mathbb{N}$ s.t. d(|G|) *then*

$\exists$ H $\in G$ where H is a subgroup and $|H| = d$

Counter-Example:

Take $a_4 =$

$\{(1), (12)(34), (13)(24), (123), .., (243)\}$

where $|A_4| = 12$

note that 8 of these 12 are of order 3

Suppose H is a group of A_4 with order 6, and take an element $a \in A_4$ that is not in H, of order 3. By Lagrange's Theorem, it has an index of 2; of most two of the subsets H, aH, a^2H are distinct. The equality of any pair of these implies a $\in H$:

$H = aH \longrightarrow a \in H$

$H = a^2H \longrightarrow a \in H$

$aH = a^2H \longrightarrow a^{-1}(aH) = a^{-1}(a^2H)$

$\longrightarrow H = aH \longrightarrow a = H$

H contains all eight elements of order 8

$\longrightarrow$ *Contradiction*!

Where does the Theorem Work?

The set of integers module 12 under addition $(\mathbb{Z}_{12}, +)$

$$\mathbb{Z}_{12} = 0, 1, 2, 3, 4, \ldots, 11$$

$H_2 = 0, 6$

$H_3 = 0, 1, 11$

$H_4 = 0, 3, 6, 9$

$H_0 = 0, 2, 4, 6, 8, 10$

.

The group of 2x2 rotational matrices of $n\frac{\pi}{2}$ about the origin under matrix multipication:

.

$$R = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} , 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

.

$$R_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

Cauchy's Theorem

This theorem is a weaker, but more robust, method for finding subgroups. It states: Let G be a finite group and let p be a prime dividing |G|. Then there is an element of order p in G.

Proof:

First, suppose that G is an abelian group.If G is generated by a single element g of order np, we can see:

$g^n \neq i.d$ and $(gn)p = i.d.$

Hence, g^n is our element.

.

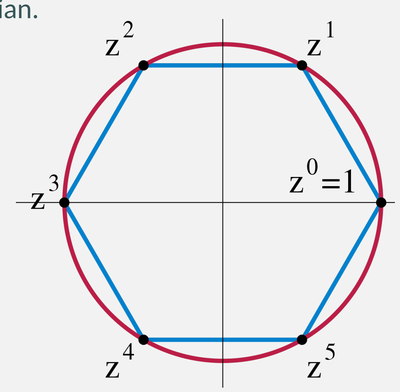
If G is not generated by a single element, we can consider a set of generating elements:

$K = \{g_1, g_2, \ldots g_n\}$

As you can see, these terms are commutative.

|

This example is isomorphic to both the 4th roots of unit and the rotational symmetries of a square. These examples work because they are abelian.



Here is another example of Abelian Groups, with the 6th Roots of unity. Seeing it visually gives a better insight into the theory.

|

Since these generating elements are commutative, the order of the group, which any selection of these generate, cannot be divisible by any prime that is not contained in the order of at least one of these generating elements.

.

Hence, the order of at least one of these generating elements of G must be divisible by p, and some power of this generating element must be the required element of order p.

.

Whilst this discovery might not seem of much significance, knowing an element of order p means you can now generate cyclical subgroups, using this element, of order p.

A Stronger Case Against the Converse

Lemma

Let S be the set of all right cosets of a subgroup H in a group G, and let $g \in G$. Then, the right multipication pg by g is a permutation on S, i.e, $pg \in A(s)$, the group of permutations on S. Moreover $g \longmapsto pg$ is a group homomorphism from $G \longmapsto A(S)$, whose kernal is contained in H.

Theorem: If $n > 4$ $k \in (1, n)$, then A_n has no subgroup of order $\frac{n!}{2k}$.

Disproving(By Contradiction)

Since A_n is simple for $n > 4$, the map $g \longmapsto pg$ defined in the lemma is a monomorphism. So the order of A_n divides $([H : G])!$

Now, as $([H : G])! = k!$, it follows that $\frac{n!}{2} > k!$

$\longrightarrow$ *Contradiction*!

Whilst this theorem certainly is the final nail in the Converse's coffin, it is very dense, and relies on some advanced actions, such as Group Homomorphisms.

Conclusion

Though, sadly, the converse case of Lagrange's Theorem is disappointingly fragile, in its failing is a rich field of study that calls upon a wide arrange of concepts that are vital for any Group Theorist in training. The topics discussed could be developed and generalised to investigate Sylow's Theorem or Hall-S Groups.

References

G.A.Miller, On an extension of Sylow's Theorem. Bull. Amer. Math. Soc., vol 4, 1898, pp.323

Joseph A. Gallian, On the Converse of Lagrange's Theorem, The American Mathematical Monthly, vol 66, 1993, pp.23

Dinesh Kurana, A note on the Converse of Lagrange's Theorem, Resonance, vol 17, pp.693